

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 18-11-2014		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 1-Oct-2012 - 30-Sep-2014	
4. TITLE AND SUBTITLE Final Report: Cloud Security: Issues and Research Directions			5a. CONTRACT NUMBER W911NF-12-1-0595		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 611102		
6. AUTHORS Sushil Jajodia			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES George Mason University 4400 University Drive, MSN 4C6 Fairfax, VA 22030 -4422			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 63027-CS-CF.1		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT We organized an invitational workshop at George Mason University on Cloud Security: Issues and Research Directions. The goals of the workshops were to establish the state of the art in the cloud security area and to set the course for future research. A multidisciplinary group of leading researchers in system and network security areas met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.					
15. SUBJECT TERMS Cloud security					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Sushil Jajodia
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 703-993-1653

Report Title

Final Report: Cloud Security: Issues and Research Directions

ABSTRACT

We organized an invitational workshop at George Mason University on Cloud Security: Issues and Research Directions. The goals of the workshops were to establish the state of the art in the cloud security area and to set the course for future research. A multidisciplinary group of leading researchers in system and network security areas met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

<u>NAME</u>	<u>PERCENT_SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT_SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME

PERCENT SUPPORTED

FTE Equivalent:

Total Number:

Names of Under Graduate students supported

NAME

PERCENT SUPPORTED

FTE Equivalent:

Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME

PERCENT SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

We organized an invitational workshop at George Mason University on Cloud Security: Issues and Research Directions. The goals of the workshops were to establish the state of the art in the cloud security area and to set the course for future research. A multidisciplinary group of leading researchers in system and network security areas met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.

Technology Transfer

We organized an invitational workshop at George Mason University on Cloud Security: Issues and Research Directions. The goals of the workshops were to establish the state of the art in the cloud security area and to set the course for future research. A multidisciplinary group of leading researchers in system and network security areas met to elaborate on the fundamental challenges facing the research community and identify promising solutions paths.

The results of the workshop were captured in the following edited book:

Sushil Jajodia, Krishna Kant, Pierangela Samarati, Anoop Singhal, Vipin Swarup, Cliff Wang, eds., *Secure Cloud Computing*, ISBN 978-1-4614-9278-8, Springer, Berlin, 2014, 343 pages..

The chapters in this book present a range of cloud computing security challenges and promising solution paths. Topics include practical considerations of cloud computing security as well as security issues related to the cloud infrastructure, data protection, computation deployment, and security state monitoring.

The book begins with two chapters focused on practical considerations of cloud computing. In Chapter 1, Chandramouli, Iorga, and Chokani describe the evolution of cloud computing and the current state of practice, followed by the challenges of cryptographic key management in the cloud. In Chapter 2, Chen and Sion present a dollar cost model of cloud computing and explore the economic viability of cloud computing with and without security mechanisms involving cryptographic mechanisms.

The next two chapters address security issues of the cloud infrastructure. In Chapter 3, Szefer and Lee describe a hardware-enhanced security architecture that protects the confidentiality and integrity of a virtual machine's memory from an untrusted or malicious hypervisor. In Chapter 4, Tsugawa et al. discuss the security issues introduced when Software-Defined Networking (SDN) is deployed within and across clouds.

Chapters 5-9 are focused on the protection of data stored in the cloud. In Chapter 5, Wang et al. present two storage isolation schemes that enable cloud users with high security requirements to verify that their disk storage is isolated from some or all other users, without any cooperation from cloud service providers. In Chapter 6, De Capitani di Vimercati, Foresti, and Samarati describe emerging approaches for protecting data stored externally and for enforcing fine-grained and selective accesses on them, and illustrate how the combination of these approaches can introduce new privacy risks. In Chapter 7, Le, Kant, and Jajodia explore data access challenges in collaborative enterprise computing environments where multiple parties formulate their own authorization rules, and discuss the problems of rule consistency, enforcement, and dynamic updates. In Chapter 8, Smith et al. address key challenges to the practical realization of a system that supports query execution over remote encrypted data without exposing decryption keys or plaintext at the server. In Chapter 9, Sun et al. provide an overview of secure search techniques over encrypted data, and then elaborate on a scheme that can achieve privacy-preserving multi-keyword text search.

The next three chapters focus on the secure deployment of computations to the cloud. In Chapter 10, Oktay et al. present a risk-based approach for workload partitioning in hybrid clouds that selectively outsources data and computation based on their level of sensitivity. The paper also describes a vulnerability assessment framework for cloud computing environments. In Chapter 11, Albanese et al. present a solution for deploying a mission in the cloud while minimizing the mission's exposure to known vulnerabilities, and a cost-effective approach to harden the computational resources selected to support the mission. In Chapter 12, Kontaxis et al. describe a system that generates computational decoys to introduce uncertainty and deceive adversaries as to which data and computation is legitimate.

The last section of the book addresses issues related to security monitoring and system resilience. In Chapter 13, Zhou presents a secure, provenance-based capability that captures dependencies between system states, tracks state changes over time, and that answers attribution questions about the existence, or change, of a system's state at a given time. In Chapter 14, Wu et al. present a monitoring capability for multicore architectures that runs monitoring threads concurrently with user or kernel code to constantly check for security violations. Finally, in Chapter 15, Hasan Cam describes how to manage the risk and resilience of cyber-physical systems by employing controllability and observability techniques for linear and non-linear systems.

Table of contents of the book is given below.

Secure Cloud Computing Table of Content

1. Cryptographic Key Management Issues and Challenges in Cloud Services
Ramswamy Chandramouli, Michaela Iorga, Santosh Chokhani
2. Costs and Security in Clouds
Yao Chen and Radu Sion

3. Hardware-enhanced Security for Cloud Computing
Jakub Szefer and Ruby B. Lee
4. Cloud Computing Security: What Changes with Software-Defined Networking?
Maurício Tsugawa, Andr ea Matsunaga, and Jos e A. B. Fortes
5. Proof of Isolation for Cloud Storage
Zhan Wang, Kun Sun, Sushil Jajodia, and Jiwu Jing
6. Selective and Fine-Grained Access to Data in the Cloud
Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati
7. Enabling Collaborative Data Authorization Between Enterprise Clouds
Meixing Le, Krishna Kant, Sushil Jajodia
8. Making Query Execution Over Encrypted Data Practical
Ken Smith, M. David Allen, Hongying Lan, and Andrew Sillers
9. Privacy-preserving Keyword Search over Encrypted Data in Cloud Computing
Wenhai Sun, Wenjing Lou, Y. Thomas Hou, and Hui Li
10. Towards Data Confidentiality and a Vulnerability Analysis Framework for Cloud Computing
Kerim Y. Oktay, Mahadevan Gomathisankaran, Murat Kantarcioglu, Sharad Mehrotra and Anoop Singhal
11. Secure Mission-Centric Operations in Cloud Computing
Massimiliano Albanese, Sushil Jajodia, Ravi Jhawar, Vincenzo Piuri
12. Computational Decoys for Cloud Security
Georgios Kontaxis, Michalis Polychronakis, and Angelos D. Keromytis
13. Towards a Data-centric Approach to Attribution in the Cloud
Wenchao Zhou
14. Software Cruising: A New Technology for Building Concurrent Software Monitor
Dinghao Wu, Peng Liu, Qiang Zeng, and Donghai Tian
15. Controllability and Observability of Risk and Resilience in Cyber-Physical Cloud Systems
Hasan Cam

Technology Transfer